DTS
DEPARTMENT OF TECHNOLOGY SERVICES

TECHNICAL ARCHITECTURE REVIEW

Project Name:	Laptop Security Encryption
Requestor:	Jim Matsumura and Michael Casey
Date of Initial Request:	October 31, 2007
Request Description:	DET Service and Support has been asked to recommend a roll out for the two main packages reviewed for Laptop Security Encryption; Guardian Edge and PGP. What should be done to convey an enterprise solution and how should DET proceed to formalize this with agency IT staff and business units. Are we going to place anything of a mandatory directive for this software or is this up to each end user or business unit to decide?
Agency or Agencies:	Enterprise
Reviewers:	Bob Woolley
ARB Acceptance Date:	
Agency Requestor Acceptance Date:	

Introduction

A recent poll by vendor Credant Technologies, one of the top laptop encryption vendors, found that 88% of employee laptops carry sensitive information; everything from patient, customer, and employee records to intellectual property, financial data, and passwords. Between business risks, security breach headlines, and regulatory compliance, there appears to be a great deal of motivation to use encryption as a last line of defense against data leaks that result from laptop theft or loss. The need for laptop encryption is driven by compliance mandates and legislative requirements (see Appendix 1), and the following reasons:

- Contractual obligations require it. Many agencies and businesses are including requirements for their partners to encrypt sensitive data in transit or at rest, especially if that data contains personal information about their customers or their employees.

- Encryption offers safe harbor from mandatory disclosure requirements, and there are regulations that require customers or employees to be informed if they have reason to believe their personal data has been compromised.

- Encryption is viewed as a best practice for information protection. Organizations are proactively applying best practices to protect sensitive data. Legislative mandates like HIPAA do not explicitly require encryption, but do require that organizations follow best practices when handling sensitive data, which often means encrypting that data.

Objectives and Scope of Review

DTS should identify alternative encryption patterns and related software for laptop data encryption that will best meet the needs of State agencies within the CIO's scope of authority. Encryption methods must protect data when it is at rest on laptop devices, but must also be considered when data is in motion over networks to which the laptop device may be connected.

Baseline of Current Architecture

Aside from testing instances, there is no significant current installed base of laptop encryption software deployed in State government. There are about 60 instances of Guardian Edge and 30 instances of PGP, and there are an additional 165 instances of PGP used for e-mail encryption. One PGP 500 user license has been purchased and is available for use.

Market Overview

Data protection for laptops is a small but growing market segment. The market began with basic encryption and has since expanded to include file encryption, external data device port controls, and rights management. Products in this space utilize strong encryption algorithms to protect information on the storage system of mobile devices such as laptops. Encryption can be invoked at the file level, or at the folder, partition, or full disk level for laptop devices. Overall, Gartner and Forrester have identified about 20 vendors of laptop encryption products. Gartner has identified the following vendors as leaders in this space in the following order:

- PointSec
- Utimaco Safeware
- Credant Technologies
- SafeBoot

PGP, Entrust, and Guardian Edge are identified as visionaries in this space with less ability to execute compared to the aforementioned vendors. Visionary vendors have made significant investments in products and support, but their reach and installed base do not compare with market leaders. That being said, any of these tools may be a useful fit for State government requirements.

Encrypting data is not simple; there are technical, administrative, and business hurdles to overcome.

- Adding encryption capabilities can be expensive. PGP has offered the State a rate of $9.00 per copy, but the cost goes well beyond initial acquisition. Administration and management, as well as development efforts required to implement encryption, are cost considerations.

- Managing encrypted data adds administrative overhead. Making sure that the right people get access to encrypted data can be complex.

- Encrypting data reduces visibility. Agencies that rely heavily on network monitoring find that encrypting data renders it unreadable to existing security measures like intrusion prevention systems (IPS) and content filtering solutions.

Encryption from an enterprise perspective is at best a mixture of endpoint solutions, each applying to specialized use cases. A holistic enterprise approach to encryption will consider encrypting:

- network communications;
- e-mail;
- databases and storage repositories;
- application data; and,
- laptops and mobile devices.

Best Practices Review

For most agencies that deal with sensitive data, some of that data ends up on employee laptops at one time or another. Hard disk encryption is a relatively quick and easy way to protect the data if the laptop falls into the wrong hands. It also provides safe harbor from mandatory disclosure requirements if personal data on a lost laptop is protected by encryption.

- **Encrypted Password Databases.** Do not rely on an ad hoc approach to encryption that depends on inherently unreliable users to decide what should be encrypted and when. This approach cannot ensure that sensitive data always gets protected, and thus cannot prove that private data was never exposed.

- **File and Folder Encryption.** Use IT-administered stored data protection, based on file/folder encryption, full-disk encryption, or some combination thereof, as deemed appropriate. File/folder encryption is also selective, but encrypts files automatically, based on defined attributes like file location, file type, or source application.

- **Full-disk Encryption.** For general purpose computers, and simplified management, encrypt everything stored on a physical disk or a logical volume. Ensure that nothing is ever written to storage without being encrypted. That includes not only sensitive user data, but also application and operating system files.

IDC has suggested that an optimally effective encryption system must be:

- centrally managed and controlled;
- rapidly deployed and maintained;
- policy driven;
- completely transparent to the user;
- easily supported by Help Desk or IT personnel;
- provide support for removable media;
- expandable, allowing new managed encryption applications to be added, as needed; and,
- extensible, enabling organizations to add managed encryption to existing enterprise applications

Emerging Technologies and Trends

Solutions in the encryption area have typically been single-function, addressing only one problem like WAN or laptop encryption. Recently, vendors have started to consolidate functionality, creating suites of encryption products that can encrypt in many use cases and use a common underlying platform for policy administration, key management, and audit.

Financial Analysis

Costs for the solutions in this report vary widely. It may be in the best interest of the State to release a multiple award RFP, since most of the key vendors in this space are not currently under contract. If the initial requirement is scaled appropriately, and some preliminary product identification has been validated, the procurement may also be possible using a request for bid approach, which would be preferable from a time and effort perspective. Some profiling of which laptop and other mobile environments need encryption is necessary before a complete financial analysis can be completed.

Security Review and Analysis

Requirements for encryption will vary, adding to security management overhead and complexity. Clearly defined security objectives will simplify product choices and deployment within agencies.

Operational and Infrastructure Analysis

IT personnel within DTS/DET will need to be trained in the solution alternatives and provided policy guidance on where to deploy laptop encryption solutions. A smaller set of defined product solutions will simplify that training and ongoing technical support issues. To affect an enterprise roll out for laptop encryption, it is advisable to limit choices for management purposes and to reduce complexity. Rollout needs to be preceded by some effective policy development that establishes when and if encryption is required.

Solution Delivery Impact and Analysis

Encryption reduces visibility and can create issues for sharing data from diverse data sources. Development can be impacted from a complexity perspective with evolving data encryption and access requirements for application users.

Agency Services Impact and Analysis

The most obvious impact to agency services is increased complexity in helping users with encryption related issues. The tool selected must be one that can be centrally managed to minimize impacts on agency services personnel and related help desk and support issues. Self management is an option with some vendors such as Guardian Edge; however, the ability to do self management is not consistent across the user base. From a conservative perspective, one has to assume a level of help desk and support requirements.

Summary and Recommendations

As mobility continues to drive the use of laptop computers, the need to protect data and mitigate the potential for system loss and theft will continue to grow in importance. Identity theft continues to proliferate, with significant personal damage to victims. Government will continue to take legislative steps that will impose significant financial penalties on enterprises responsible for any disclosure of personal data. The State of Utah needs to take proactive steps to establish policies and processes to prevent the accidental or deliberate disclosure of data and the associated risk to individuals and to government as a trusted entity when such disclosures occur. As an overall observation, laptop encryption will add complexity, cost, support issues, and will also impact laptop performance to some extent, so it should be implemented only where it is needed. Unfortunately, problems often come from unanticipated and often policy non-compliant sources, so the risk level is only mitigated in a limited way. Policy for encryption becomes very important.

> ***Recommendation #1:*** **Encryption solutions must adapt to future requirements with minimal deployment issues.** The choice of encryption technology should take into consideration future requirements without the need for complete redeployment, retraining, and redundant administration and support costs.
>
> ***Recommendation #2:*** **Select a single platform for laptop encryption.** A single vendor simplifies training and support and encourages opportunities to specialize for DTS staff.

***Recommendation #3:* Provide an encryption solution with a range of capabilities, not just the easiest to install.** Select solutions that will support file and folder level encryption as well as volume or drive level encryption, but minimize the number of solutions deployed. While having folder level capability may be desirable, it does induce additional levels of user management risk.

***Recommendation #4:* Understand the impact of encryption.** Assess the overall impact of the encryption solution decision on end users, IT, and support and Help Desk staff. Anticipate issues and develop strategies for mitigating them. Existing pilot work with the desktop group should be evaluated for lessons learned.

***Recommendation #5:* Mandatory encryption aligned with business needs.** Align business requirements. Use of encryption technologies must be mandatory to comply with agency regulatory mandates as business drivers. Policy development is required, and must address conditions when encryption is essential. Information security policy 5000-1700, and the conversion to Administrative Rule, should be reviewed to ensure that these issues are addressed.

***Recommendation #6:* Consistent enforcement of encryption policies.** The encryption solution selected must be able to enforce encryption policies consistently across a range of encryption configurations.

***Recommendation #7:* Use an encryption tool that is optimal for laptops.** Encryption solutions need to be optimal for the task at hand. Implement a single tool for laptop enterprise encryption. The solution for laptop encryption may not be the appropriate solution for external storage device control, or for PDA encryption. One solution may not work for everything.

Of the product solutions available, and considering the size of existing installed bases, PGP appears to be a solution that could be deployed consistently and meet both general and point specific encryption requirements for laptops. Selection of a secondary solution should be approached with some caution to reduce complexity, management, and support issues. A secondary solution is more appropriately focused on solving other business problems such as self management, external storage, or PDA encryption, although PGP does address both of these functions.

Self management of encryption solutions do not appear on anyone’s best practice list, although self management functionality is attractive from an administrative cost perspective. Self management is particularly attractive when encryption policies have not been defined. This approach generally results in an unevenly applied solution that may have limited benefit to the State.

Forrester has suggested that encryption is often used as “a blunt tool to provide the illusion of security.” Without identifying the data that needs to be encrypted and when, and without strong key management, encryption offers little security. In many cases there are more cost-effective ways of providing security before resorting to encryption, like conventional access controls and process improvements. Moreover, there are business processes around identity management and data classification that should be in place before encryption can be implemented effectively and efficiently.

Summary of Agency Review Comments

No comments were received on this TA Review. Subsequent research on the Open Enterprise Server (OES) TA Review disclosed that Novell also has a centrally managed endpoint security product called Novell ZenWorks Endpoint Security Manager. This product is available under the existing Master License Agreement with Novell. The product is priced at $34.50 per user for initial license purchase, and $8.50 per year for maintenance. This product was not reviewed by the team that made the initial comparisons of encryption alternatives. The software integrates with the OES 2 environment and eDirectory. It is a re-branded product from Senforce. Features of the management console include the following:[1]

- ***Personal Firewall****:* Standard configurable personal firewall software.
- ***Wireless Security****:* Centrally controls when, how, and where users are allowed to connect. Wi-Fi connectivity can be limited to authorized and known access points, minimum encryption strength, or can be disabled completely if necessary.
- ***Data Encryption****:* Secures data stored on the endpoint and on removable media, encrypting files so they can only be read by authorized users. Protects sensitive information on lost or stolen mobile computers.
- ***USB Security****:* Prevents intentional or inadvertent transmission of data to removable storage devices. Storage devices can be placed in read-only mode or fully disabled, while the endpoint hard drive and all network drives remain accessible and operational.
- ***Application Control****:* Ensures that only approved applications are run on State IT assets—create black lists, or enforce applications to run (i.e., VPN or antivirus) prior to network connection.

[1] *Novell ZenWorks Endpoint Security Management* at http://www.novell.com///products/zenworks/endpointsecuritymanagement

- ***Client Self Defense**:* Protects the endpoint by ensuring that the security client cannot be altered, hacked, or uninstalled.

- ***Port Control**:* Controls connectivity via LAN, modem, Bluetooth™, Infrared, 1394 (Firewire™), and serial and parallel ports.

- ***Alerts Monitoring**:* Provides a scalable and simple method for creating, distributing, enforcing, and monitoring security policies on endpoint devices, without forcing users to make security decisions or adjust settings.

The fairly comprehensive nature of this endpoint security product, and the fact that it is already available under an existing contract, would seem to warrant additional evaluation.

References

Girard, John, with Ray Wagner and Vic Wheatman, *Magic Quadrant for Mobile Data Protection, 1H06*, Gartner RAS Core Research Note G00141980, August 29, 2006.

Novell ZenWorks Endpoint Security Management at
http://www.novell.com///products/zenworks/endpointsecuritymanagement

Kolodgy, Charles J., and Gerry Pintal, *Securing Laptops with Full Disk Encryption*, IDC Whitepaper, January 2007.

Penn, John, and Thomas Raschke, *Information Leak Prevention, Q4 2006*, Forrester Wave, December 15, 2006.

Phifer, Lisa, *Emerging Technologies*, Information Security Magazine, July 2007.

_________, *Encryption Strategies for Preventing Laptop Data Leaks*, Network Security Tactics, August 20, 2007.

Stamp, Paul, with Jonathan Penn and Alissa Dill, *Adopting an Enterprise Approach to Encryption*, Forrester Trends, March 6, 2007

Appendix 1: Federal Privacy Legislation in the United States

Date Introduced	Bill Number	Bill Name	Purpose
March 3, 2005	H.R. 1069	Notification of Risk to Personal Data Act	Requires that consumers be notified when the security of their information is breached.
March 3, 2005	S.500/H.R. 1080	Information Protection and Security Act	Directs the FTC (Federal Trade Commission) to promulgate rules that set standards for information brokers and then to report back to Congress.
April 11, 2005	S.751	Notification of Risk to Personal Data Act	Requires notification to consumers in the event of unauthorized access to sensitive personal information.
April 12, 2005	S.768	Comprehensive Identity Theft Prevention Act	Requires notice of security breaches, imposes obligations on data merchants to keep information secure, and restricts the use, sale, and posting of Social Security numbers as part of a comprehensive privacy and anti-ID theft measure.
October 25, 2005	HR 4127	The Financial Data Protection Act	Designed to protect consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information and to provide for nationwide notice in the event of a security breach.
September 29, 2005	S.1789	Personal Data Privacy and Security Act of 2005	Introduced to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.
December 21, 2005	S 2169	The Financial Data Protection Act	Amends the Fair Credit Reporting Act to provide for secure financial data and for other purposes.
February 8, 2006	H.R. 4709	Telephone Records and Privacy Protection Act of 2006	Amends Title 18, United States Code to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.
July 17, 2006	H. R. 5820	Federal Agency Data Privacy Protection Act	Intends to increase the security of sensitive data maintained by the federal government.